

Re: debugging encrypted part of isakmp

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-01/0056.html>

From: Andriy Gapon (*avg_at_icyb.net.ua*)

Date: 01/14/05

Date: Fri, 14 Jan 2005 16:44:19 +0200

To: Bruce M Simpson <bms@spc.org>

on 14.01.2005 16:07 Bruce M Simpson said the following:

> *On Fri, Jan 14, 2005 at 11:54:36AM +0200, Andriy Gapon wrote:*

> *man 8 isakmpd:*

>

> *%%%*

> *–L Enable IKE packet capture. When this option is given, isakmpd*

> *will capture to file an unencrypted copy of the negotiation pack–*

> *ets it is sending and receiveing. This file can later be read by*

> *tcpdump(8) and other utilities using pcap(3).*

> *%%%*

>

The problem is it is not isakmpd.

Here's more information: I am trying to reverse–engineer asymmetric xauth/mode cfg exchange between third–party VPN/ipsec client and server.

I know all configuration parameters for both, but I don't have any access to internal workings. At this point, I also have too little information to successfully emulate either side, but I know what phase1 mode they use and what key material they have.

So, I am looking for the easiest way to decrypt isakmp packets using both packet data and information like pre–shared keys, certificates etc.

--

Andriy Gapon

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"